PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-150550
(43)Date of publication of application : 23.05.2003

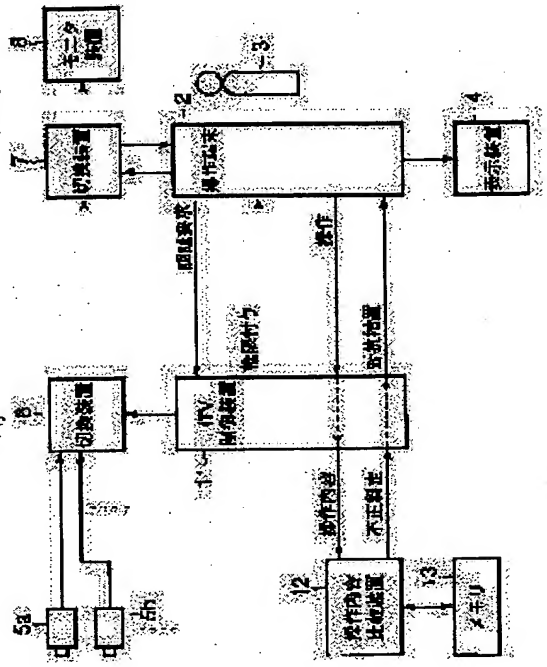
(51)Int.Cl. G06F 15/00
G06F 1/00

(21)Application number : 2001-349154
(22)Date of filing : 14.11.2001

(71)Applicant : TOSHIBA CORP
(72)Inventor : ENOMOTO HIDEAKI

(54) INFORMATION PROCESSING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the lengthening of the period of an illicit access by successively judging whether or not the operator is a formal operator even after log-on is normally executed by using a formal password.
SOLUTION: An operation content comparing device 12 is connected to an ITV control device 11, and the operation content of a specific period is prestored in a memory 13. The operation content comparing device 12 determines whether or not to be normal operation by comparing the present operation content with the operation content stored in the memory 13 after executing log-on in a system. When it is judged that operation is not the normal operation, a countermeasure is executed by setting an illicit level of 'small', 'medium', and 'large'. A warning is displayed in the level of 'small', and when illicit operation continues further, a level is transferred to the level of 'medium' to display the effect of making illicit access, and log-out is forcibly executed. When the illicit operation continues by executing the log-on again with the same password, the level is transferred to the level of 'large' to forcibly execute the log-out, and an account of the operator 3 is set unusable.



LEGAL STATUS

[Date of request for examination] 18.10.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－150550
（P2003－150550A）
(43)公開日　平成15年５月23日(2003.5.23)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ａ　５Ｂ０８５
1/00	３７０	1/00	３７０Ｅ

審査請求　未請求　請求項の数５　ＯＬ　（全５頁）

(21)出願番号　特願2001－349154(P2001－349154)

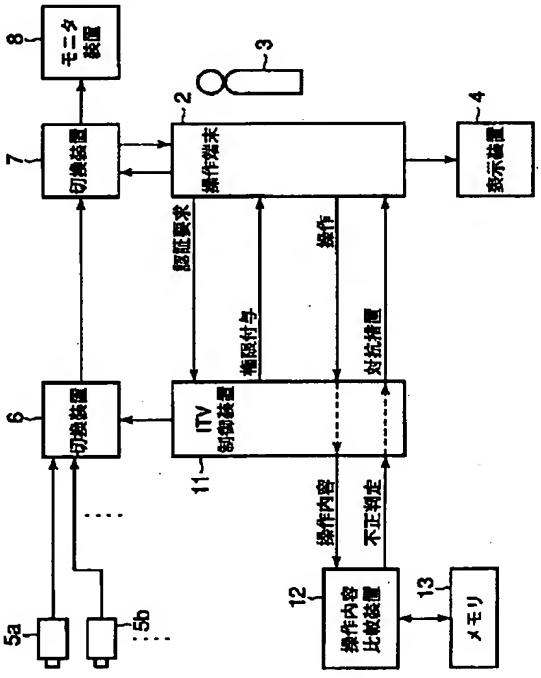
(22)出願日　平成13年11月14日(2001.11.14)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　榎本　秀明
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B085 AE03 AE06 AE15

(54)【発明の名称】　情報処理システム

(57)【要約】
【課題】正式なパスワードを使用して正常にログオンされた後においても、正式な操作者かどうかを逐次判断して不正アクセスの長期化を防止する。
【解決手段】ＩＴＶ制御装置１１に操作内容比較装置１２を接続し、メモリ１３に予め一定期間の操作内容を記憶する。操作内容比較装置１２は、システムへのログオンが行なわれた後、現在の操作内容とメモリ１３に記憶している操作内容とを比較して通常操作かどうかを判断する。通常操作ではないと判断された場合、不正レベル「小」、「中」、「大」を設定して対抗措置を実施する。レベル「小」では、警告表示を行ない、更に不正操作が続く場合はレベル「中」に移行し、不正アクセスが行なわれた旨の表示を行なうと共に強制的にログアウトさせる。再度同じパスワードでログオンして不正操作が続く場合、レベル「大」に移行し、強制的にログアウトすると共に操作者３のアカウントを使用不可に設定する。



1

【特許請求の範囲】

【請求項１】　パスワードを入力して正式な操作者を確認する情報処理システムにおいて、操作アカウント毎に一定期間の操作内容を記憶する記憶手段と、前記操作者による現在の操作と前記記憶手段に記憶されている操作内容とを比較し、現在の操作内容が通常操作と異なる場合に不正操作が行なわれたものと判断する判断手段と、前記判断手段により不正操作が行なわれたものと判断された場合にその操作内容に応じて対抗措置を実施する手段とを具備したことを特徴とする情報処理システム。

【請求項２】　パスワードを入力して正式な操作者を確認する情報処理システムにおいて、操作アカウント毎に許容する操作内容を予め記憶する記憶手段と、前記操作者による現在の操作と前記記憶手段に記憶されている操作内容とを比較し、現在の操作内容が通常操作と異なる場合に不正操作が行なわれたものと判断する判断手段と、前記判断手段により不正操作が行なわれたものと判断された場合にその操作内容に応じて対抗措置を実施する手段とを具備したことを特徴とする情報処理システム。

【請求項３】　前記対抗措置を実施する手段は、判断手段により不正操作が行なわれたものと判断された場合にその操作内容に応じて不正レベルを「小」、「中」、「大」に設定し、最初は不正レベル「小」から実施し、不正操作が続けられた場合に順次不正レベル「中」、「大」の対抗措置を実施することを特徴とする請求項１又は２記載の情報処理システム。

【請求項４】　前記対抗措置を実施する手段は、判断手段により不正操作が行なわれたものと判断された場合にその操作内容に応じて不正レベルを「小」、「中」、「大」に設定し、不正レベル「小」では操作端末画面上に警告表示を行ない、その後、不正操作が続く場合に不正レベル「中」に移行して操作端末画面上に不正アクセス表示を行なって強制的にログアウトし、更に再度同じパスワードでログオンして不正操作が続けられた場合に不正レベル「大」に移行して強制的にログアウトすると共にその操作者のアカウントを使用不可に設定することを特徴とする請求項１又は２記載の情報処理システム。

【請求項５】　前記対抗措置を実施する手段は、判断手段により不正操作が行なわれたものと判断された場合に、その操作内容がシステム上保安性の高い部分に関連する操作かどうかを判断し、保安性の高い部分に関連する操作の場合には最初からレベル「中」あるいはレベル「大」の対抗措置を実施することを特徴とする請求項３又は４記載の情報処理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、端末操作者に対する認証機能を備えた情報処理システムに関する。

【０００２】

2

【従来の技術】従来、例えばプラントの稼働状態や工場の各施設等を監視するシステムとして、図４に示すようなＩＴＶ（industrial television）システムが用いられている。

【０００３】図４において、１はＩＴＶ制御装置、２は上記ＩＴＶ制御装置１の操作端末である。この操作端末２は、操作者３によって操作されるもので、その操作に対応した情報を表示装置４に表示する。

【０００４】上記ＩＴＶ制御装置１は、操作端末２の操作に従って監視カメラ５ａ、５ｂ、…の切換装置６を制御する。上記監視カメラ５ａ、５ｂ、…は、例えばプラントや工場等の監視対象領域に設置される。上記監視カメラ５ａ、５ｂ、…により撮影された監視画像は、切換装置６により選択され、更に切換装置７を介してモニタ装置８へ送られる。上記切換装置７は、操作端末２によって切換え制御され、監視画像をモニタ装置８へ出力すると共に、操作端末２側にも出力できるようになっている。すなわち、操作端末２は、モニタ装置８に表示される監視画像を切換装置６を介して取り込み、自己の表示装置４に表示できるようになっている。

【０００５】上記のように構成されたＩＴＶシステムでは、ＩＴＶ制御装置１に予め操作者３に対するパスワードを登録しておき、操作開始時にパスワードの正否を認証するようになっている。すなわち、操作端末２は、操作者３が操作を開始する際、表示装置４にパスワードの入力画面を表示し、操作者３がパスワードを入力すると、ＩＴＶ制御装置１に対してパスワードが正しいかどうかの認証要求を行なう。ＩＴＶ制御装置１は、入力されたパスワードと予め登録されているパスワードとを比較認証し、正式なパスワードであれば操作端末２への操作入力を許可し、操作者３に対して操作権限を付与する。

【０００６】

【発明が解決しようとする課題】上記従来のＩＴＶシステムでは、操作開始時にパスワードの認証処理を行なっているので、正式なパスワードを知らない不正操作者による入力を拒否することができる。

【０００７】しかし、従来のＩＴＶシステムでは、例えばパスワードを盗まれたり、あるいは不正に解読された場合、それを使ってシステムに正常にログオンされてしまうと、操作者が不正な権限利用を行なっていることを見分けられず、長期間の不正アクセスを許してしまうという問題があった。

【０００８】本発明は上記の課題を解決するためになされたもので、正式なパスワードを使用して正常にログオンされた後においても、正式な操作者かどうかを逐次判断して不正アクセスの長期化を防止することができる情報処理システムを提供することを目的とする。

【０００９】

【課題を解決するための手段】本発明に係る情報処理シ

ステムは、パスワードを入力して正式な操作者を確認する情報処理システムにおいて、操作アカウント毎に一定期間の操作内容を記憶する記憶手段と、前記操作者による現在の操作と前記記憶手段に記憶されている操作内容とを比較し、現在の操作内容が通常操作と異なる場合に不正操作が行なわれたものと判断する判断手段と、前記判断手段により不正操作が行なわれたものと判断された場合にその操作内容に応じて対抗措置を実施する手段とを具備したことを特徴とする。

【００１０】上記の構成によれば、正式なパスワードを使用してシステムに正常にログオンした後も、操作者による操作を記憶・分析し、正式な操作者かどうかを逐次判断して不正アクセスに対する対抗措置を実施することができる。従って、正式なパスワードが盗まれたり、不正に解読された場合でも、不正アクセスの長期化を確実に防ぐことができ、システムのセキュリティを向上することができる。

【００１１】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態を説明する。図１は、本発明の一実施形態に係るＩＴＶシステムの構成を示すブロック図である。図１において、１１はＩＴＶ制御装置、２は上記ＩＴＶ制御装置１１の操作端末である。この操作端末２は、操作者３によって操作されるもので、その操作に対応した情報を表示装置４に表示する。

【００１２】上記ＩＴＶ制御装置１１は、操作端末２の操作に従って監視カメラ５ａ、５ｂ、…の切換装置６を制御する。上記監視カメラ５ａ、５ｂ、…は、例えばプラントや工場等の監視対象領域に設置される。上記監視カメラ５ａ、５ｂ、…により撮影された監視画像は、切換装置６により選択され、更に切換装置７を介してモニタ装置８へ送られる。上記切換装置７は、操作端末２によって切換え制御され、監視画像をモニタ装置８へ出力すると共に、操作端末２側にも出力できるようになっている。すなわち、操作端末２は、モニタ装置８に表示される監視画像を切換装置６を介して取り込み、自己の表示装置４に表示できるようになっている。

【００１３】上記ＩＴＶ制御装置１１には、予め操作者３に対するパスワードを登録しておき、操作開始時にパスワードの正否を認証し、正式なパスワードであれば操作端末２への操作入力を許可し、操作者３に対して操作権限を付与する機能を備えている。更に、ＩＴＶ制御装置１１には、操作内容比較装置１２が接続される。この操作内容比較装置１２は、各アカウント毎の操作内容を記憶するためのメモリ１３を備えている。上記操作内容比較装置１２は、操作アカウント毎に一定期間の操作内容をメモリ１３に記憶し、それを基準にして現在の操作内容と比較することにより不正アクセスを検出してＩＴＶ制御装置１１へ出力する。ＩＴＶ制御装置１１は、操作内容比較装置１２により不正アクセスが検出された場合、その程度に応じて不正レベル「小」、「中」、「大」を設定すると共に、例えば「不正表示」、「ログアウト」、「アカウント使用不可」等の対抗措置を実施する。

【００１４】次に、上記実施形態における不正アクセスの検出動作を図２及び図３に示すフローチャートを参照して説明する。図２は、操作開始時のパスワード入力に対する処理動作を示すフローチャートである。操作者３は、操作を開始する際、操作端末２よりパスワードを入力する（ステップＡ１）。操作端末２は、パスワードが入力されたことを検知すると（ステップＡ２）、ＩＴＶ制御装置１１に対して認証要求を行なう。ＩＴＶ制御装置１１は、上記認証要求により認証処理を開始し（ステップＡ３）、入力されたパスワードと予め登録されているパスワードとを比較し、入力されたパスワードが正式のものであるか否かを判断する（ステップＡ４）。入力されたパスワードが間違っていれば、その旨を表示装置４に表示して再度の入力に備える。また、入力されたパスワードが正しい場合には、ＩＴＶ制御装置１１から操作端末２へ操作権限を付与する情報を操作端末２へ送り、その後の操作入力を受付ける（ステップＡ５）。

【００１５】上記のように正常にログオンした場合、その後の操作者３による操作端末２の操作内容、例えば普段どの映像を見るか、どの制御を行なうか、よく使用するボタンはどれか等について、操作アカウント毎に一定の期間例えば１ヶ月の間、ＩＴＶ制御装置１１から操作内容比較装置１２へ送ってメモリ１３に記憶する。

【００１６】次に、上記操作権限が操作者３に与えられた後の処理動作を図３に示すフローチャートに従って説明する。上記のように操作者３の通常の操作内容を操作内容比較装置１２のメモリ１３に記憶した後、操作者３が操作端末２を操作すると（ステップＢ１）、その操作内容はＩＴＶ制御装置１１から操作内容比較装置１２へ送られる。操作内容比較装置１２は、操作者３の操作内容を予めメモリ１３に記憶している操作内容と操作アカウント毎に比較し、通常行なわれている操作かどうかを判断し（ステップＢ２）、その判断結果をＩＴＶ制御装置１１に通知する。上記操作内容比較装置１２において、現在の操作が通常操作であると判断された場合、ＩＴＶ制御装置１１は、その操作内容に対応した処理を実行し（ステップＢ３）、ステップＢ１に戻って次の入力に備える。

【００１７】また、操作内容比較装置１２において、現在の操作が通常行なわれていない、あるいは操作者３の職務から外れるようなものであると判断された場合、ＩＴＶ制御装置１１は、その不正レベルに応じた対抗措置を実施する。

【００１８】先ず、その操作がシステム上保安性の高い部分に関連する操作かどうかを判断し（ステップＢ４）、保安性の高い部分に関連する操作でなければ不正

レベルが「小」に設定されているかどうか（ステップＢ５）、更には「中」に設定されているかどうかを判断する（ステップＢ６）。不正レベルが「小」、「中」の何れにも設定されていなければ、不正レベルを「小」に設定し（ステップＢ７）、操作ミスか機器の誤動作である可能性も考慮して、操作端末２の表示装置４に例えば「誤った操作が行なわれましたので、注意して下さい。」等の警告を表示する（ステップＢ８）。その後、ステップＢ１に戻って次の入力操作に備える。

【００１９】また、上記ステップＢ５において、既に不正レベル「小」が設定されていると判断された場合、すなわち、上記ステップＢ７で不正レベル「小」が設定された後、更に不正と思われる操作が続く場合には、ステップＢ５からステップＢ９に進んで不正レベルを「中」に設定し、表示装置４に例えば「不正な操作が行なわれました。」等の不正表示を行ない（ステップＢ１０）、強制的にログアウトさせる（ステップＢ１１）。

【００２０】また、上記ステップＢ６において、既に不正レベル「中」が設定されていると判断された場合、すなわち、上記ステップＢ９で不正レベルが「中」に設定されて強制的にログアウトされた後、再度同じパスワードでログオンして不正と思われる操作が続く場合には、ステップＢ６からステップＢ１２に進んで不正レベルを「大」に設定し、強制的にログアウトさせる（ステップＢ１３）。更に、その操作者のアカウントを使用不可に設定し（ステップＢ１４）、処理を終了する。

【００２１】また、上記ステップＢ４において、入力操作がシステム上保安性の高い部分に関連する操作であると判断された場合には、直ちにステップＢ１２に進み、最初から不正レベル「大」の措置を実施する。なお、上記ステップＢ４において、入力操作がシステム上保安性の高い部分に関連する操作であると判断された場合、ステップＢ９に進んで不正レベル「中」の措置を実施するようにしてもよい。

【００２２】上記実施形態に示すように正常にログオンした後も、操作者３による操作を記憶・分析し、正式な操作者かどうかを逐次判断し、不正アクセスに対する対抗措置を実施するようにしたので、正式なパスワードが盗まれたり、不正に解読された場合でも、不正アクセスの長期化を防ぐことができ、システムのセキュリティを向上することができる。

【００２３】なお、上記実施形態では、操作者３の一定期間の操作内容をメモリ１３に記憶するようにしたが、その他、例えば通常行なう操作内容を予め特定してメモリ１３に記憶するようにしてもよい。すなわち、操作者３の操作内容は、システムの構成あるいは各操作者の職務等によって特定することができるので、予め許容できる範囲の操作内容をメモリ１３に記憶させることが可能である。

【００２４】また、上記実施形態では、ＩＴＶ制御装置１１に対して操作内容比較装置１２を外部接続する場合について示したが、ＩＴＶ制御装置１１の内部に操作内容比較装置１２及びメモリ１３を設けても良いことは勿論である。

【００２５】また、上記実施形態では、ＩＴＶシステムに実施した場合について示したが、その他のシステムであっても、パスワードを使用して正式な操作者を確認する情報処理システムにおいて実施し得るものである。

【００２６】

【発明の効果】以上詳記したように本発明によれば、パスワードを使用して正式な操作者を確認する情報処理システムにおいて、システムに正常にログオンした後も、操作者による操作を記憶・分析し、正式な操作者かどうかを逐次判断し、不正アクセスに対する対抗措置を実施するようにしたので、正式なパスワードが盗まれたり、不正に解読された場合でも、不正アクセスの長期化を防ぐことができ、システムのセキュリティを向上することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るＩＴＶシステムの構成を示すブロック図。

【図２】同実施形態における操作開始時のパスワード入力に対する処理動作を示すフローチャート。

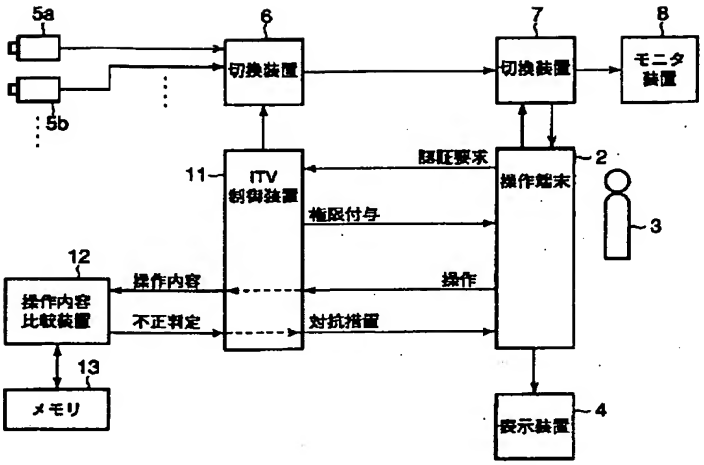
【図３】同実施形態において、正常にログオンした後の不正アクセスに対する処理動作を示すフローチャート。

【図４】従来のＩＴＶシステムの構成を示すブロック図。

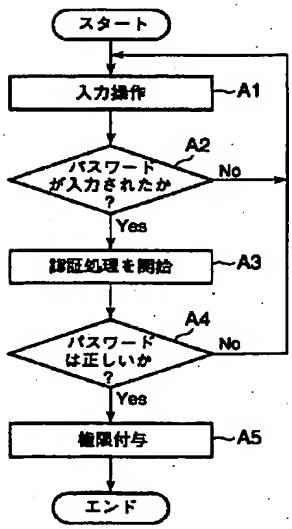
【符号の説明】

２…操作端末
３…操作者
４…表示装置
５ａ、５ｂ、…、…監視カメラ
６、７…切換装置
８…モニタ装置
１１…ＩＴＶ制御装置
１２…操作内容比較装置
１３…メモリ

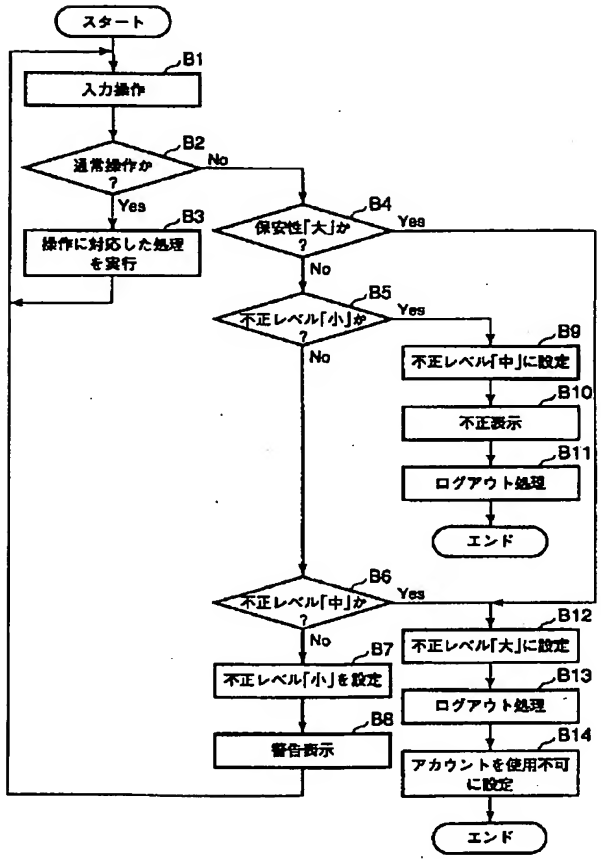
【図１】


5a
6
7
8
切換装置
切換装置
モニタ装置
5b
11
ITV制御装置
認証要求
操作端末
2
権限付与
3
12
操作内容
操作
操作内容比較装置
不正判定
対抗措置
13
メモリ
表示装置
4

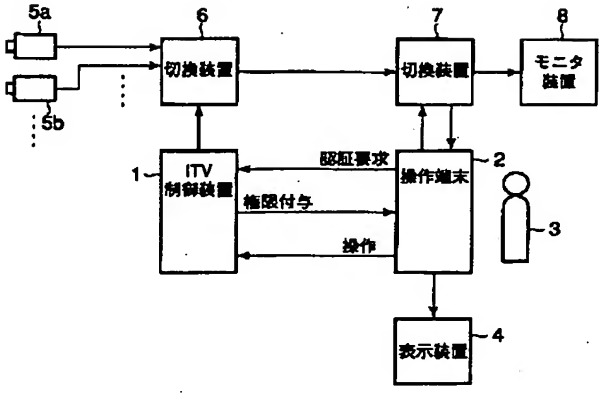
【図２】


スタート
入力操作
A1
パスワードが入力されたか？
A2
No
Yes
認証処理を開始
A3
パスワードは正しいか？
A4
No
Yes
権限付与
A5
エンド

【図３】


スタート
B1
入力操作
B2
通常操作か？
No
Yes
B3
操作に対応した処理を実行
B4
保安性「大」か？
Yes
No
B5
不正レベル「小」か？
Yes
No
B9
不正レベル「中」に設定
B10
不正表示
B11
ログアウト処理
エンド
B6
不正レベル「中」か？
Yes
No
B12
不正レベル「大」に設定
B7
不正レベル「小」を設定
B13
ログアウト処理
B8
警告表示
B14
アカウントを使用不可に設定
エンド

【図４】


5a
6
7
8
切換装置
切換装置
モニタ装置
5b
1
ITV制御装置
認証要求
操作端末
2
権限付与
3
操作
表示装置
4